REMARKS/ARGUMENTS

Prior to entry of this amendment, claims 1-65 were pending in this application. Claims 55, 60 and 63 have been amended, claims 61 and 64 have been canceled, and no claims have been added herein. Therefore, claims 1-60, 62, 63 and 65 remain pending in this application. Applicants respectfully request reconsideration of these claims, as amended, for at least the reasons presented below.

35 U.S.C. § 102 Rejection, Olden

Claims 1-65 were previously rejected under 35 U.S.C. § 102(e) as being anticipated by U. S. Patent No. 6,460,141 to Eric M. Olden (hereinafter "Olden"). The Applicants respectfully submit the following arguments pointing out significant differences between claims 1-60, 62, 63 and 65 submitted by the Applicants and Olden.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP 2131 citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Applicants respectfully argue that Olden fails to disclose each and every claimed element. For example, Olden fails to disclose, either expressly or inherently, acquiring user identification information from an authentication system by an authorization system that is separate from the first authentication system. In another example, Olden fails to disclose, either expressly or inherently, an authentication system external to and access system and relying on the authentication system for authenticating a user. In yet another example, Olden fails to disclose, either expressly or inherently, an access system that provides for using of one or more internal authentication systems and relies on one or more external authentication systems for accessing a resource.

As stated previously, Olden is directed to "[a] security and access management system [that] provides unified access management to address the specific problems facing the deployment of security for the Web and non-Web environment." Olden, Abstract. Also as stated previously, under the system of Olden, the authorization server performs both authentication and authorization services, while the entitlements server merely maintains the entitlements database, which holds data to be used by the authorization server. That is, the authorization server of Olden performs both the authentication (determining whether the user is valid, *see* Olden, Fig. 29) and authorization (determining whether the user is authorized to access a particular URL, based on entitlements in the entitlements database, *see* Olden, Fig. 28). In other words, Olden is similar to the integrated solutions described in the background of the application. Application, p. 2, ll. 10-11. However, as an integrated system including both authentication and authorization functions, Olden does not, for example, provide the ability to use a legacy authentication system (i.e., a separate authentication system).

Independent claim 1 recites in part "acquiring user identification information from a first authentication system, said user identification information is associated with a request from a first user to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said first authentication system; relying on said first authentication system for authenticating said first user" and "performing, at said authorization system, authorization services for said request to access said first resource based on said identity profile associated with said user identification information." Other independent claims, i.e., claims 15, 21, 32, 42, and 50 each recite similar limitations. That is, these claims and their dependent claims recite an authorization system and an authentication system that are two separate systems, one of which (the authentication system) is responsible for verifying the identity of the user, and the other of which (the authorization system) is responsible for determining whether the user is authorized to access the requested resource.

The Office Action maintains that it interprets "the term 'separate' as not necessarily physical separation. " However, mere "temporal separation" does not teach an authorization system that is separate from an authentication system. That is, the independent claims clearly define an authorization system and an authentication system that are distinct, separate systems. Olden does not teach or suggest such separate systems. Rather, Olden discloses only an integrated system including both authentication and authorization functions. Furthermore, even if the term "separate" might mean "temporal separation," "virtual separation," or "software module separation," nothing in Olden teaches or suggests any separation whatsoever (however defined) between the authentication and authorization functions. Rather, Olden specifically teaches an integrated system similar to the systems described in the background of the present application that performs an integrated authentication/authorization process.

Independent claim 38 recites in part "acquiring user identification information from a first authentication system external to said access system, said user identification information is associated with a request from a first user to access a first resource, [and] relying on said first authentication system for authenticating said first user." Other independent claims, i.e., claims 46 and 55 each recite similar limitations. That is, these claims and their dependent claims recite an access system that uses an external authentication system for authenticating a user. Olden does not teach or suggest such an external authentication system. Rather, Olden discloses only an integrated system including only internal authentication and authorization functions.

Independent claim 26 recites in part "receiving, at an access system, configuration information for a first resource, said access system provides for using of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said configuration information provides an indication to said access system to rely on a first external authentication system for said first resource." Other

independent claims, i.e., claims 46 and 55 each recite similar limitations. That is, these claims and their dependent claims recite an access system that uses both internal and external authentication systems. Olden does not teach or suggest such both internal and external authentication systems. Rather, Olden discloses only an integrated system including only internal authentication and authorization functions.

For at least these reasons, claims 1-60, 62, 63 and 65 are believed to be distinct from Olden. Therefore, the Applicants respectfully request that the rejection be withdrawn and the claims allowed.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

Date: June 12, 2006

William J. Daley
Reg. No. 52,471

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, CA 94111-3834
Tel: 303-571-4000 (Denver office)
Fax: 303-571-4321 (Denver office)

WJD/sbm

60794975 v1